UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
**United States Patent and Trademark Office**
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/720,214 | 11/25/2003 | Ming-Fong Yeh | P24609 | 4973 |

7055 7590 03/19/2008
GREENBLUM & BERNSTEIN, P.L.C.
1950 ROLAND CLARKE PLACE
RESTON, VA 20191

| EXAMINER | |
|---|---|
| HENNING, MATTHEW T | |
| **ART UNIT** | **PAPER NUMBER** |
| 2131 | |
| **NOTIFICATION DATE** | **DELIVERY MODE** |
| 03/19/2008 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

gbpatent@gbpatent.com
pto@gbpatent.com

| | | |
|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/720,214 | **Applicant(s)**<br>YEH ET AL. |
| | **Examiner**<br>MATTHEW T. HENNING | **Art Unit**<br>2131 |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *25 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 November 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *2/25/04 3/18/04 5/18/06*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

This action is in response to the communication filed on 11/25/2003.

## DETAILED ACTION

Claims 1-39 have been examined.

### *Title*

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

### *Information Disclosure Statement*

The information disclosure statement(s) (IDS) submitted on 2/25/2004, 3/18/2004, 5/18/2006 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statements.

### *Drawings*

The drawings are objected to because Fig. 14d is labeled “Fig. 14b”. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR

1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### *Specification*

Applicant is reminded of the proper language and format for an abstract of the disclosure.

*The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.*

*The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.*

The abstract of the disclosure is objected to because:

“The present invention provides” can be implied and therefore should be removed from the abstract.

Correction is required. See MPEP § 608.01(b).

The disclosure is objected to because of the following informalities: It appears that the “continuous sequence 01 01 01 02 02 02 03 04" on page 20 line 4 may not be consistent with the description on page 19-20. It appears that it should read “01 01 01 02 03 03 03 04”.

Appropriate correction is required.

### *Claim Objections*

Claims 1-22, 27-28, and 39 are objected to because of the following informalities:

Claims 1-21 and 27-28 recite “the attribute definition field”, but there are a plurality of these fields, and thus the limitation should read "each attribute definition field".

Claims 1, 5, 13, 15, 16, and 27 recite "that matches attribute of" which is not grammatically correct. This should read "that matches an attribute of" or "that matches attribute information of".

Appropriate correction is required.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

*A person shall be entitled to a patent unless –*

*(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.*

Claims 7, 9, 11, and 29-36 are rejected under 35 U.S.C. 102(e) as being anticipated by Tan (US Patent Number 6,490,353).

Regarding claim 7, Tan disclosed a data encryption method, the method comprising the following steps: Step A: constructing encryption definition data containing a plurality of encryption algorithm module indicators (See Tan Col. 8 Lines 15-24); Step B: inputting digital data to be encrypted (See Tan Col. 8 Lines 38-54); Step C: from the encryption definition data, selecting at random an encryption algorithm module indicator (See Tan Col. 10 Lines 37-55); Step D: with the selected encryption algorithm module indicator as a guide, controlling encryption processing of the inputted digital data (See Tan Col. 10 Lines 37-55); and Step E:

appending decryption information to the digital data that has undergone encryption processing for subsequent output (See Tan Col. 4 Lines 7-23).

Regarding claim 9, Tan disclosed that the encryption definition data constructed in step A includes a plurality of encryption algorithm module combinations, each of the encryption algorithm module combinations including an encryption algorithm module indicator and an authentication algorithm module indicator, an encryption algorithm module combination being selected at random from the retrieved encryption definition data in step C, the selected encryption algorithm module combination being used as a guide for controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data in step D (See Tan Col. 7 Lines 13-25).

Regarding claim 11, Tan disclosed A data encryption method, the method comprising the following steps: Step A: constructing an encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator (See Tan Col. 7 Lines 13-25 and Col. 8 Lines 15-24); Step B: constructing encryption definition data which includes a plurality of encryption module database indexes (See Tan Col. 8 Lines 15-24); Step C: inputting digital data to be encrypted(See Tan Col. 8 Lines 38-54); Step D: from the encryption definition data, selecting at random an encryption module database index (See Tan Col. 10 Lines 37-55); Step E: according to the retrieved encryption module database index, selecting an entry of record from the encryption module database (See Tan Col. 10 Lines 37-55); Step F: with the selected entry of record as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data (See Tan Col. 10 Lines 37-55); and

Step G: appending decryption information to the digital data that has undergone encryption for subsequent output (See Tan Col. 4 Lines 7-23).

Regarding claim 29, Tan disclosed a data decryption method, the method comprising the following steps: Step A: inputting digital data to be decrypted (See Tan Col. 10 Line 64 – Col. 11 Line 4); Step B: inspecting whether the digital data includes a decryption algorithm module indicator and, in the affirmative, retrieving the decryption algorithm module indicator or, in the negative, setting the data to be decrypted as equivalent to inputted data for subsequent processing in step D (See Tan Col. 13 Lines 4-39 and Col. 8 Lines 3-6); Step C: with the retrieved decryption algorithm module indicator as a guide, controlling decryption processing of the inputted digital data (See Tan Col. 13 Lines 4-39); and Step D: outputting the digital data that has undergone decryption (See Tan Col. 13 Lines 4-39).

Regarding claim 31, Tan disclosed a data decryption method, the method comprising the following steps: Step A: constructing a decryption module database for storing a plurality of entries of records of data, each of the entries of records being a decryption algorithm module indicator (See Tan Col. 4 Lines 7-23); Step B: inputting digital data to be decrypted (See Tan Col. 10 Line 64 – Col. 11 Line 4); Step C: inspecting whether the digital data includes a decryption module database index and, in the affirmative, retrieving the decryption module database index or, in the negative, setting the data to be decrypted as equivalent to inputted data for subsequent processing in step F (See Tan Col. 13 Lines 4-39 and Col. 8 Lines 3-6); Step D: with the retrieved decryption module database index as a guide, selecting an entry of record from the decryption module database (See Tan Col. 13 Lines 4-39); Step E: with the selected entry of record as a guide, controlling decryption processing of the inputted digital data (See Tan Col. 13

Lines 4-39); and Step F: outputting the digital data that has undergone decryption (See Tan Col. 13 Lines 4-39).

Regarding claim 33, Tan disclosed a data decryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after decryption processing thereof (See Tan Col. 10 Line 64 – Col. 11 Line 4), the apparatus further comprising: an inspecting portion for inspecting whether the data inputted via the input portion includes a decryption algorithm module indicator and, in the affirmative, retrieving the decryption algorithm module indicator or, in the negative, transmitting the inputted data directly to the output portion (See Tan Col. 13 Lines 4-39 and Col. 8 Lines 3-6); and a decryption processing portion for controlling decryption processing of the inputted digital data using the decryption algorithm module indicator retrieved by the inspecting portion as a guide (See Tan Col. 13 Lines 4-39).

Regarding claims 30, 32, and 34, Tan disclosed that the inspecting portion inspects whether the data inputted via the input port ion includes a decryption algorithm module combination, the decryption algorithm module combination including a decryption algorithm module indicator and an authentication algorithm module indicator, and, in the affirmative, retrieves the decryption algorithm module combination or, in the negative, transmitting directly the inputted data to the output portion, the decryption processing portion controlling the decryption processing, including the type of decryption and the type of authentication, of the inputted digital data using the decryption algorithm module indicator retrieved by the inspecting portion as a guide (See Tan Col. 7 Lines 13-25).

Regarding claim 35, Tan disclosed a decryption module database for storing a plurality of entries of records of data, each of the entries of records containing a decryption algorithm module indicator, the inspecting portion inspecting whether the data inputted via the input portion includes a decryption module database index and, in the affirmative, retrieving the decryption module database index and further retrieving an entry of record from the decryption module database using the index or, in the negative, transmitting directly the inputted data to the output portion, the decryption processing portion controlling the decryption processing of the inputted digital data using the entry of record retrieved by the inspecting portion as a guide (See Tan Col. 4 Lines 7-23 and Col. 13 Lines 4-39).

Regarding claim 36, Tan disclosed that the decryption module database stores a plurality of entries of records of data, each of the entries of records containing a decryption algorithm module indicator and an authentication algorithm module indicator, the decryption processing portion controlling decryption processing, including the type of decryption and the type of authentication, using the entry of record retrieved by the inspecting portion as a guide (See Tan Col. 7 Lines 13-25).

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to*

*which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 1, 3, 5, 13-15, 18, 20, 22, 25, 28, and 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tan (US Patent Number 6,490,353).

Regarding claim 1, Tan disclosed a data encryption method (See Tan Fig. 13), the method including the following steps: Step A: constructing a security class database for storing a plurality of entries of records of data (See Tan Col. 8 Lines 18-24 pool of securithms), each of the entries of records including a corresponding encryption definition field, the encryption definition field including a plurality of encryption algorithm module indicators (See Tan Col. 7 Line 65 – Col. 8 Line 37); Step B: inputting digital data to be encrypted (See Tan Col. 8 Lines 38-54); Step C: from the security class database, retrieving the corresponding encryption definition data (See Tan Col. 8 Lines 15-25 Library); Step D: from the retrieved encryption definition data, selecting at random an encryption algorithm module indicator (See Tan Col. 10 Lines 37-55); Step E: with the selected encryption algorithm module indicator as a guide, controlling encryption processing of the inputted digital data (See Tan Col. 10 Lines 37-55); and Step F: appending decryption information to the digital data that has undergone encryption processing for subsequent output (See Tan Col. 4 Lines 7-23), but Tan failed to disclose each record also including a data attribute description field; or finding a data attribute description that matches attribute of the digital data. However, Tan did disclose that the choice of complexity of the securithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the securithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have included an indication of the complexity level of each securithm in the pool. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each securithm when determining which securithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 5, Tan disclosed a data encryption method, the method comprising the following steps: Step A: constructing an encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator (See Tan Col. 8 Lines 18-24 pool and Col. 7 Lines 14-25); Step C: inputting digital data to be encrypted (See Tan Col. 8 Lines 38-54); Step D: finding a data attribute description that matches attribute of the digital data, and retrieving the corresponding encryption definition data (See Tan Col. 8 Lines 15-25 Library); Step E: from the retrieved encryption definition data, selecting at random an encryption module database index (See Tan Col. 10 Lines 37-55); Step F: according to the retrieved encryption module database index, selecting an entry of record from the encryption module database (See Tan Col. 10 Lines 37-55); Step G: with the selected entry of record as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data (See Tan Col. 10 Lines 37-55); and Step H: appending decryption information to the digital data that has undergone encryption processing for subsequent output (See Tan Col. 4 Lines 7-23), but Tan failed to disclose Step B: constructing a security class database for storing a plurality of entries of records of data, each of the entries of records containing a data attribute description field and a corresponding encryption definition field, the encryption definition field including a plurality of encryption module database indexes. However, Tan did disclose that the choice of complexity of the securithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the securithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have included an indication of the complexity level of each securithm in the pool. This would have been obvious <u>because</u> the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each securithm when determining which securithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 13, Tan disclosed a data encryption method, the method comprising the following steps: Step A: constructing a security class database for storing a plurality of entries of records of data, each of the entries of records containing a corresponding encryption definition field, the encryption definition data field being an encryption algorithm module indicator (See Tan Col. 8 Lines 15-25); Step B: inputting digital data to be encrypted (See Tan Col. 8 Lines 38-54); Step C: retrieving the encryption algorithm module indicator of the corresponding encryption definition field (See Tan Col. 8 Lines 15-25); Step D: with the selected encryption algorithm module indicator as a guide, controlling encryption processing of the inputted digital data (See Tan Col. 10 Lines 37-55); and Step E: appending decryption information to the digital data that has undergone encryption processing for subsequent output(See Tan Col. 4 Lines 7-23), but Tan failed to disclose each of the entries of records containing a data attribute description field; or from the security class database, finding a data attribute description that matches attribute of the digital data. However, Tan did disclose that the choice of complexity of the securithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the securithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have included an indication of the complexity level of each securithm in the pool. This would have been obvious <u>because</u> the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each securithm when determining which securithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 15, Tan disclosed a data encryption method, the method including the following steps: Step A: constructing an encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator (See Tan Col. 8 Lines 15-25); Step C: inputting digital data to be encrypted (See Tan Col. 8 Lines 38-54); Step D: retrieving the encryption module database index from the corresponding encryption definition field (See

Tan Col. 8 Lines 15-25); Step E: with the retrieved encryption module database index as a guide, selecting an entry of record from the encryption module database (See Tan Col. 8 Lines 38-54); Step F: with the selected entry of record as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data (See Tan Col. 8 Lines 38-54); and Step G: appending decryption information to the digital data that has undergone encryption processing for subsequent output (See Tan Col. 4 Lines 7-23) however, Tan failed to disclose Step B: constructing a security class database for storing a plurality of entries of records of data, each of the entries of records containing a data attribute description field and a corresponding encryption definition field, the encryption definition data field being an encryption module database index; or Step D: from the security class database, finding a data attribute description that matches attribute of the digital data, and retrieving the encryption module database index from the corresponding encryption definition field. However, Tan did disclose that the choice of complexity of the securithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the securithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have included an indication of the complexity level of each securithm in the pool, and selecting the securithm based upon an appropriate complexity level required for the input data. This would have been obvious <u>because</u> the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each securithm when determining which securithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 16, Tan disclosed a data encryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after encryption processing thereof, the apparatus further comprising: a security class database for storing a plurality of entries of records of data, a corresponding encryption definition field, the encryption definition field including a plurality of encryption algorithm module indicators (See Tan Col. 8 Lines 15-25); an attribute inspecting portion for finding from the security class database a data attribute description that matches attribute of the digital data sent from the inspecting portion and for transmitting the corresponding encryption definition data to a encryption selecting portion (See Tan Col. 8 Lines 15-25); the encryption selecting portion, which selects at random an encryption algorithm module indicator from the retrieved encryption definition data (See Tan Col. 8 Lines 38-54); and an encryption processing portion for controlling encryption processing of the inputted digital data using the encryption algorithm module indicator selected by the encryption selecting portion as a guide (See Tan Col. 8 Lines 38-54), but Tan failed to specifically disclose each of the entries of records containing a data attribute description field; an inspecting portion for inspecting and separating the data inputted via the input portion into parameter data or digital data; a parameter processing portion for updating the security class database with the parameter data sent from the inspecting portion. However, Tan did disclose that the choice of complexity of the securithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the securithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have included an indication of the complexity level of each securithm in the pool, to have automatically determined the input data type and selecting the securithm based upon an appropriate complexity level required for the input data type. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each securithm when determining which securithms were complex enough for the policy regarding the data type being encrypted.

Regarding claim 23, Tan disclosed a data encryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after encryption processing thereof, the apparatus further comprising: a encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator (See Tan Col. 8 Lines 15-25); a encryption selecting portion for selecting at random an entry of record from the encryption module database (See Tan Col. 8 Lines 38-54); and an encryption processing portion for controlling encryption processing of the inputted digital data using the entry of record selected by the encryption selecting portion as a guide (See Tan Col. 8 Lines 38-54), but Tan failed to specifically disclosed an inspecting portion for inspecting and separating the data inputted via the input portion into parameter data or digital data; a parameter processing portion for updating the encryption module database using the parameter data from the inspecting portion. However, Tan did disclose that the choice of complexity of the securithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the securithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have included an indication of the complexity level of each securithm in the pool, and selecting the securithm based upon an appropriate complexity level required for the input data. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each securithm when determining which securithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 27, Tan disclosed a data encryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after encryption processing thereof, the apparatus further comprising: a security class database for storing a plurality of entries of records of data, each of the entries of records containing a corresponding encryption definition field, the encryption definition field being an encryption algorithm module indicator (See Tan Col. 8 Lines 15-25); and the encryption processing portion for controlling encryption processing of the inputted digital data using the encryption algorithm module indicator selected as a guide (See Tan Col. 8 Lines 38-54), but Tan failed to specifically disclose a security class database for storing a plurality of entries of records of data, each of the entries of records containing a data attribute description field and an inspecting portion for inspecting and separating the data inputted via the input portion into parameter data or digital data; a parameter processing portion for updating the security class database with the parameter data from the inspecting portion; an attribute inspecting portion for finding from the security class database a data attribute description that matches attribute of the digital data sent from the inspecting portion and for transmitting the corresponding encryption definition data to an encryption processing portion. However, Tan did disclose that the choice of complexity of the securithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the securithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have included an indication of the complexity level of each securithm in the pool, and selecting the securithm based upon an appropriate complexity level required for the input data. This would have been obvious <u>because</u> the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each securithm when determining which securithms were complex enough for the policy regarding the data being encrypted.

Regarding claims 3, 14, 18, 25, and 28, Tan disclosed that the encryption definition field in the security class database constructed in step A is an encryption algorithm module combination, the encryption algorithm module combination including an encryption algorithm module indicator and an authentication algorithm module indicator, data of an encryption algorithm module combination of the corresponding encryption definition field being retrieved in the step C of finding from the security class database the data attribute description that matches the attribute of the digital data, the selected encryption algorithm module combination being used in step D as a guide for controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data (See Tan Col. 7 Lines 13-25).

Regarding claim 20, Tan disclosed an encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator(See Tan Col. 7 Lines 13-25); the encryption definition field of the security class database including a plurality of encryption module database indexes(See Tan Col. 8 Lines 15-25); the encryption selecting portion selecting at random an encryption module database index from the retrieved encryption definition data and, according to the retrieved encryption module database index, and selecting an entry of record from the encryption module database(See Tan Col. 8 Lines 38-54); the encryption processing portion using the entry of record selected by the encryption selecting portion as a guide to control encryption processing, including the type of encryption and the type of authentication, of the inputted digital data(See Tan Col. 8 Lines 38-54).

Regarding claim 22, Tan disclosed that the parameter processing portion updates the security class database and the encryption module database using the parameter data sent from the inspecting portion (See Tan Col. 8 Lines 15-25).

Regarding claim 37, Tan disclosed the claimed decryption system including inspecting whether the digital data includes a decryption module database index and, in the affirmative, retrieving the decryption module database index and further retrieving an entry of record from the decryption module database using the index and, in the negative, transmitting directly the inputted data to the output portion (See Tan Col. 8 Lines 3-25 and Col. 13 Lines 4-39) but failed to specifically disclose a parameter processing portion for updating the decryption module database using parameter data, the inspecting portion inspecting and separating the data inputted via the input portion into parameter data or digital data and, if the inputted data is parameter data, transmitting the same to the parameter processing portion and, if the inputted data is digital data. However, Tan did disclose that the choice of complexity of the securithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the securithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have included an indication of the complexity level of each securithm in the pool, and selecting the securithm based upon an appropriate complexity level required for the input data. This would have been obvious <u>because</u> the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each securithm when determining which securithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 38, Tan disclosed the decryption module database stores a plurality of entries of records of data, each of the entries of records containing a decryption algorithm module indicator and an authentication algorithm module indicator, the decryption processing portion controlling decryption processing, including the type of decryption and the type of authentication, of the inputted digital data using the entry of record retrieved by the inspecting portion as a guide (See Tan Col. 7 Lines 13-25 and Col. 13 Lines 4-39).

Claims 2, 4, 6, 8, 10, 12, 17, 19, 21, 24, 26, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tan as applied to claims 1, 5, 7, 11, 16, 23, and 27 above, and further in view of Kim et al. (US Patent Number 6,499,127) hereinafter referred to as Kim.

Tan disclosed randomly selecting one algorithm from a set of algorithms randomly and that the encryption definition field in the security class database constructed in step A includes a plurality of encryption algorithm module indicators and corresponding proportions adopted thereby (See Tan Col. 8 Lines 15-25 and Col. 9 Lines 34-40), but failed to specifically disclose an encryption algorithm module indicator being selected from the retrieved encryption definition data in step D according to each of the encryption algorithm module indicators and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

Kim teaches a method for selecting a number in a range randomly comprising determining the size of the range, generating a random number, and taking the random number modulo the size of the range (See Kim Col. 23 Paragraph 1).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kim in the random algorithm system of Tan by selecting the algorithm randomly from the seed by generating a random number and then taking the random number MOD the number of entries in the seed. This would have been obvious because the ordinary person skilled in the art would have been motivated to select the algorithm randomly as taught by Tan.

Regarding claim 39, Tan disclosed that the parameter processing portion updates the security class database and the encryption module database using the parameter data sent from the inspecting portion (See Tan Col. 8 Lines 15-25).

***Conclusion***

Claims 1-39 have been rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Examiner, Art Unit 2131

/Christopher A. Revak/
Primary Examiner, Art Unit 2131